July 6, 2018

Via Electronic Submission

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue N.W.
Washington, DC 20551

Re: **Docket No. OP-1607; Policy on Payment System Risk and Expanded Real-time Monitoring**

Dear Ms. Misback,

The Clearing House Payments Company[1] (**TCH**) appreciates the opportunity to provide comments to the Board of Governors of the Federal Reserve System (**Board**) in response to the potential change to the Federal Reserve Policy on Payment System Risk. The change would provide for real-time monitoring of all Fedwire Funds transfers (**Fedwire transfers**) and rejection of transfers that would breach the Fedwire sender's net debit cap (together, **Expanded Monitoring**). Under current practices, a net debit cap is generally used in ex-post monitoring of Federal Reserve accounts but not applied as a "hard" cap that results in rejection of debit entries to accounts. By limiting overdrafts in Federal Reserve accounts caused by Fedwire transfers, Expanded Monitoring is intended to protect the Federal Reserve Banks from potential losses and serve as a backstop in the event a bank sends errant or fraudulent[2] Fedwire transfers.

TCH supports the reduction of risk posed to Federal Reserve Banks and Fedwire senders by Fedwire transfers that would breach a bank's net debit cap. However, as more fully discussed below, we encourage the Board to consider alternatives to payment rejection that would be consistent with the objectives of Expanded Monitoring. We also suggest that the Board engage with Fedwire senders to explore other tools that might be employed to prevent and detect fraud.

Alternatives to Rejection. In its consideration of Expanded Monitoring the Board analyzed 2016 Fedwire data to determine what impact Expanded Monitoring would have had on Fedwire transfers that

[1] The Clearing House is a payments company that is owned by the largest commercial banks and dates back to 1853. The company owns and operates core payments system infrastructure in the United States, including a new, ubiquitous, real-time payment system. The company is the only private-sector ACH and wire operator in the United States, clearing and settling nearly $2 trillion in U.S. dollar payments each day, representing half of all commercial ACH and wire volume.

[2] In the context of this letter, fraudulent transfers refers to transfers resulting from the compromise of a Fedwire sender's systems (i.e. endpoint compromise).

year. The analysis indicated that only .003%, or 3,990, of the 133 million Fedwire transfers sent in 2016 would have been rejected had Expanded Monitoring been in place. While this is a small number of Fedwire transfers, we agree with the Board's observation that historically high levels of reserve balances have decreased the need for intraday credit for some banks.[3] Hence, the Board's analysis of 2016 Fedwire transfers may not be a reliable measure of the impact of Expanded Monitoring in a lower reserve environment. With lower reserves, the likelihood increases that Fedwire senders may breach their net debit caps. Hence, we are uncertain how impactful Expanded Monitoring may be over time.

Additionally, we think that operational error is more likely to be the cause of a net debit cap breach than fraud. And in the event of such an operational error that would cause rejection of Fedwire transfers under Expanded Monitoring, the Fedwire sender will likely need to resubmit the Fedwire transfer or transfers that were rejected in order to execute its customers' payment orders. However, resubmission of Fedwire transfers is an exception process for most banks. The process will create operational burden for Fedwire senders and likely slow the resubmission of the transfers, impacting bank customers and inter-bank liquidity flows. We note that if a Fedwire sender is close to its net debit cap, relatively low value Fedwire transfers may reject and during peak volume periods the Fedwire sender may have tens or hundreds of Fedwire payments suddenly rejected, which would amplify the operational burden and delay of resubmission.

We think the Board should consider other actions that could be taken under Expanded Monitoring that will both achieve the Board's objective of reducing risks to Reserve Banks and Fedwire senders and be less disruptive to banks in lower reserve environments and when they experience operational errors. For example, as an alternative to rejecting Fedwire transfers that would breach the Fedwire sender's net debit cap, the Reserve Banks could pend the transfers and require the Fedwire sender to authorize release of the transfers (and to fund the transfers, if at the time of authorization the transfers would otherwise cause a breach of the bank's net debit cap). However, depending upon the time of day, pended payments may be more problematic than rejected payments.

Fedwire senders will be better served if the Reserve Banks' actions under Expanded Monitoring are more tailored to the banks' operational needs. Because the Federal register notice did not consider options other than rejection, if such options can be implemented by the Reserve Banks, we suggest that the Board and Reserve Banks engage in direct dialogue with Fedwire users to determine the optimal actions to be taken under Expanded Monitoring. It may be useful for the Reserve Banks to conduct a survey of the operational capabilities of banks as part of such a dialogue.

Other Tools. While recognizing that Expanded Monitoring is an improvement over current controls, we are not certain that it is a meaningful tool for detecting or preventing fraud given how large net debit caps can be. If a Fedwire sender's systems were compromised and multiple fraudulent Fedwire transfers were being sent, the bank would have very significant financial exposure by the time a transfer breached the bank's net debit cap. We hope that the Board will engage with Fedwire senders to explore other potential tools that would be better suited to address fraud.

*****

[3] Policy on Payment System Risk and Expanded Real-time Monitoring (May 8, 2018), footnote 9.

Thank you for your consideration of these comments. If you have any questions or wish to discuss this letter, please do not hesitate to contact me.

Yours very truly,

Alaina Gimbert
Senior Vice President & Associate General Counsel
The Clearing House Payments Company L.L.C.
Alaina.Gimbert@theclearinghouse.org